

# Exhibit 2

**U.S. Patent No. 8,165,024 (“’024 Patent”)****Exemplary Accused Product**

Solarwinds products, including at least each of the following products (and their variations) infringe at least Claim 1 of the ’024 Patent: Solarwinds’s Network Performance Monitor. The infringement chart below is based on the Solarwinds’s Network Performance Monitor (NPM) solution (“Network Performance Monitor (NPM)”), which is exemplary of the infringement of the ’024 Patent.

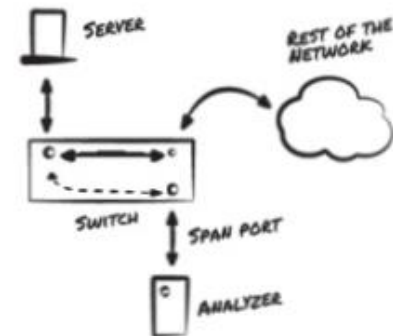
Claims	Network Performance Monitor (NPM)
<p>[1pre] A method of processing packets sent from a source node to a destination node, the method comprising:</p>	<p>NPM processes packets sent from a source node to a destination node.</p> <div data-bbox="766 649 1890 1282"> <p><i>Deep Packet Analysis</i></p> <ul style="list-style-type: none"> <li>Also known as Deep packet Inspection (DPI)</li> <li>Capturing (by making a copy of) and analyzing the contents of network packets that flow between clients &amp; servers</li> <li>Packets are typically captured using a 'TAP' or switch port 'mirroring' or 'spanning'</li> </ul> <p>Diagram: SERVER ↔ SWITCH ↔ REST OF THE NETWORK (cloud). SWITCH → ANALYZER (via SPAN PORT).</p> <p>solarwinds</p> </div> <p><a href="https://www.slideshare.net/SolarWinds/solar-winds-deep-packet-inspection-for-quality-of-experience-monitoring">https://www.slideshare.net/SolarWinds/solar-winds-deep-packet-inspection-for-quality-of-experience-monitoring</a></p>

	<p><b>Identify traffic by application</b></p> <p>Analyze and identify network traffic by capturing, analyzing, and monitoring packets. SolarWinds' packet capture software identifies over 1,200 applications, calculates application and network response time, data volume and transactions, and categorizes traffic into types, volumes, classification, and risk.</p> <p><a href="https://www.solarwinds.com/network-performance-monitor/use-cases/packet-capture">https://www.solarwinds.com/network-performance-monitor/use-cases/packet-capture</a></p>
[1a] receiving a packet sent from the source node to the destination node;	NPM receives a packet sent from the source node to the destination node.

## Deep Packet Analysis

Clip slide

- Also known as Deep packet Inspection (DPI)
- Capturing (by making a copy of) and analyzing the contents of network packets that flow between clients & servers
- Packets are typically captured using a 'TAP' or switch port 'mirroring' or 'spanning'



solarwinds

<https://www.slideshare.net/SolarWinds/solar-winds-deep-packet-inspection-for-quality-of-experience-monitoring>

## Identify traffic by application

Analyze and identify network traffic by capturing, analyzing, and monitoring packets. SolarWinds' packet capture software identifies over 1,200 applications, calculates application and network response time, data volume and transactions, and categorizes traffic into types, volumes, classification, and risk.

<https://www.solarwinds.com/network-performance-monitor/use-cases/packet-capture>

<p>[1b] associating the packet with an active flow by accessing information in the packet;</p>	<p>NPM associates the packet with an active flow by accessing information in the packet.</p> <p>The <b>packet analyzer</b> can automatically classify network traffic according to category and identify the associated risk level. The scanner can categorize traffic based on destination server IP addresses, ports used, and measurement of the total and relative volumes of traffic for each type. With deep packet inspection, you can identify excess levels of non-business traffic that may need to be filtered or eliminated. You can also identify traffic flowing over a network link or traffic to specific servers or applications, enabling informed capacity management.</p> <p><a href="https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection">https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection</a></p> <p><b>Identify traffic by application</b></p> <p>Analyze and identify network traffic by capturing, analyzing, and monitoring packets. SolarWinds' packet capture software identifies over 1,200 applications, calculates application and network response time, data volume and transactions, and categorizes traffic into types, volumes, classification, and risk.</p> <p><a href="https://www.solarwinds.com/network-performance-monitor/use-cases/packet-capture">https://www.solarwinds.com/network-performance-monitor/use-cases/packet-capture</a></p>
--	---

## Traffic distribution analysis

Clip slide

- Categorization & measurement of network traffic types based on IP addresses, ports and protocols
- Identify business vs. non-business and potentially malicious traffic

Protocol	% Packets	Packets	% Bytes
Frame	100.00 %	9076	100.00 %
Ethernet	100.00 %	9050	100.00 %
Internet Protocol Version 4	100.00 %	9050	100.00 %
Internet Control Message Protocol	6.65 %	602	5.38 %
Transmission Control Protocol	93.35 %	8448	94.61 %
Hypertext Transfer Protocol	13.43 %	1206	66.62 %
Line-based text data	0.29 %	26	0.41 %
Media Type	0.02 %	2	0.04 %
Tabular Data Stream	28.91 %	2616	25.72 %
Unassembled Fragmented Packet	13.99 %	1266	19.64 %
Tabular Data Stream	0.87 %	79	1.57 %
Short Frame	0.18 %	16	0.34 %

© 2014 SOLARWINDS WORLDWIDE, LLC. ALL RIGHTS RESERVED.

solarwinds

<https://www.slideshare.net/SolarWinds/solar-winds-deep-packet-inspection-for-quality-of-experience-monitoring>

[1c] performing deep packet inspection (DPI) to identify an application associated with the active flow by analyzing at least one other packet;

NPM performs deep packet inspection (DPI) to identify an application associated with the active flow by analyzing at least one other packet.

	<p>The <b>packet analyzer</b> can automatically classify network traffic according to category and identify the associated risk level. The scanner can categorize traffic based on destination server IP addresses, ports used, and measurement of the total and relative volumes of traffic for each type. With deep packet inspection, you can identify excess levels of non-business traffic that may need to be filtered or eliminated. You can also identify traffic flowing over a network link or traffic to specific servers or applications, enabling informed capacity management.</p> <p><a href="https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection">https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection</a></p> <p>Deep packet inspection is a technique for monitoring network and application traffic at the packet level. Using response time metrics for packets sent between clients and servers, admins can regulate traffic flows and differentiate between network issues and application issues.</p> <p><a href="https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection">https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection</a></p>
--	--

	<p>With SolarWinds® deep packet inspection software, you can calculate response times for over 1,200 applications right out of the box. You're able to monitor metrics for all relevant applications, including Skype, SQL Server, Facebook, and more. Because the deep packet inspection tools focus on the metavalues of the applications and not the packets themselves, you won't take up space in the database with traffic data you don't need to see. You can also go beyond the limited capabilities of programs like Wireshark and achieve a full view across every network interface.</p> <p><a href="https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection">https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection</a></p>
[1d] determining a classification for the packet based on characteristics of the identified application;	NPM determines a classification for the packet based on characteristics of the identified application.



## Deep packet Inspection & Quality of Experience

Clip slide

- New in NPM version 11
- Easy-to-deploy software deep packet inspection and analysis sensors
- Quality of Experience dashboard for a quick summary of network and application performance metrics
  - Visual presentation of over 1200 application (i.e. Skype®, SQL, facebook®, etc...) response times, classification (messaging, database, social, etc...), categorization (business vs. non-business), and risk profile
  - Visual presentation of network response time
  - Graphical display of traffic volume and transaction count

© SOLARWINDS WORLDWIDE, LLC. ALL RIGHTS RESERVED.



solarwinds

<https://www.slideshare.net/SolarWinds/solar-winds-deep-packet-inspection-for-quality-of-experience-monitoring>

Q - How many application signatures are supported?

A - Over 1200

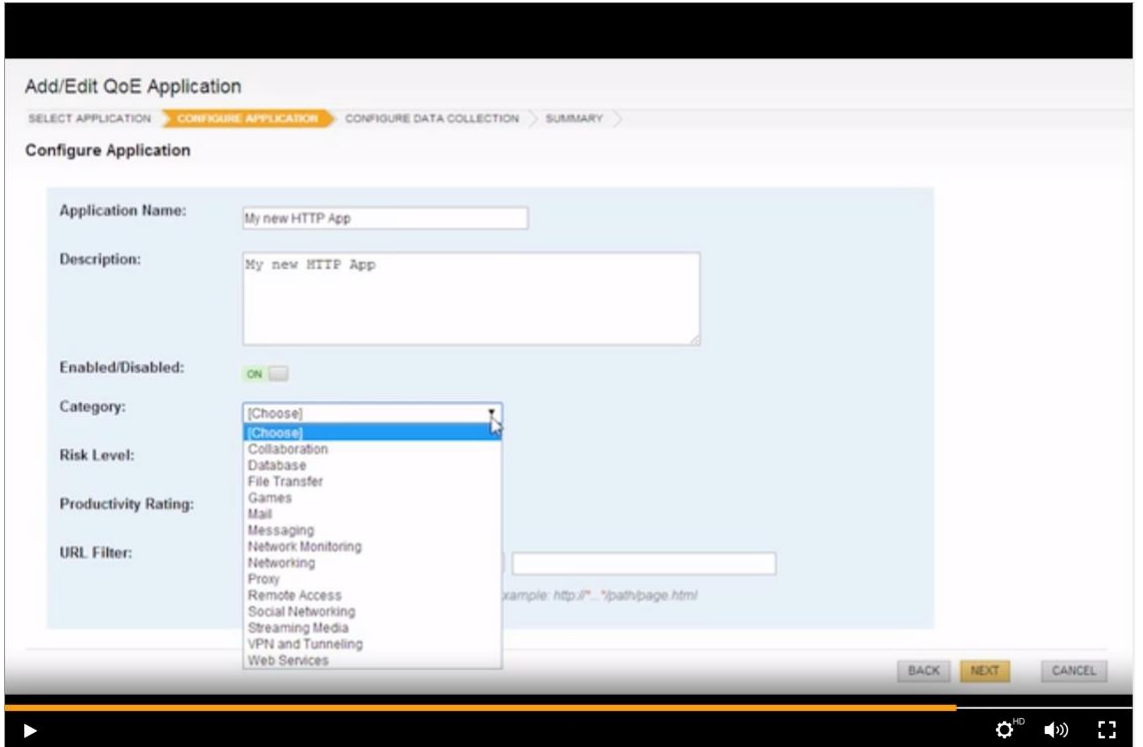
Q - Are these signatures updated dynamically through product updates?

A - Yes

Q - Can custom applications be defined?

A - Yes, custom HTTP applications can be defined.

<https://thwack.solarwinds.com/t5/Product-Blog/Deep-Packet-Inspection-and-Analysis-FAQs/ba-p/509409>

	 <p><a href="https://support.solarwinds.com/SuccessCenter/s/article/Deep-Packet-Inspection-Video">https://support.solarwinds.com/SuccessCenter/s/article/Deep-Packet-Inspection-Video</a> at 3:00.</p>
[1e] inserting information identifying the classification into the packet;	NPM inserts information identifying the classification into the packet.



## Analyze over 1,200 applications

Calculate response times for all relevant applications and determine the impact on user experience.



## Classify network traffic

Classify and restrict network traffic as needed and identify associated risk levels.

<https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection>

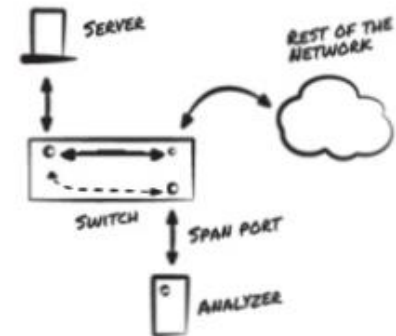
The **packet analyzer** can automatically classify network traffic according to category and identify the associated risk level. The scanner can categorize traffic based on destination server IP addresses, ports used, and measurement of the total and relative volumes of traffic for each type. With deep packet inspection, you can identify excess levels of non-business traffic that may need to be filtered or eliminated. You can also identify traffic flowing over a network link or traffic to specific servers or applications, enabling informed capacity management.

	<p><a href="https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection">https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection</a></p> <p>The network packet analysis tools in NPM are designed to not only capture and analyze packet data, but they can also automatically classify network traffic. The platform is built to display network traffic information according to category and provide an estimate of the risk level associated with this traffic. The analyzer categorizes traffic according to elements like source or destination IP address, port usage, application type, and volume. Admins can also identify how traffic flows over a specific network link or to servers or applications. Armed with these insights, admins can make informed decisions about capacity planning. The network packet analysis tools in NPM can make it easier to filter out worrisome levels of non-business traffic.</p> <p><a href="https://www.solarwinds.com/network-performance-monitor/use-cases/packet-analyzer">https://www.solarwinds.com/network-performance-monitor/use-cases/packet-analyzer</a></p>
<p>[1f] forwarding the packet, including the information identifying the classification, towards the destination node such that a downstream device is enabled to perform processing of the packet by extracting the classification from the packet.</p>	<p>NPM forwards the packet, including the information identifying the classification, towards the destination node such that a downstream device is enabled to perform processing of the packet by extracting the classification from the packet.</p>

## Deep Packet Analysis

Clip slide

- Also known as Deep packet Inspection (DPI)
- Capturing (by making a copy of) and analyzing the contents of network packets that flow between clients & servers
- Packets are typically captured using a 'TAP' or switch port 'mirroring' or 'spanning'



solarwinds

<https://www.slideshare.net/SolarWinds/solar-winds-deep-packet-inspection-for-quality-of-experience-monitoring>

The [packet analyzer](#) can automatically classify network traffic according to category and identify the associated risk level. The scanner can categorize traffic based on destination server IP addresses, ports used, and measurement of the total and relative volumes of traffic for each type. With deep packet inspection, you can identify excess levels of non-business traffic that may need to be filtered or eliminated. You can also identify traffic flowing over a network link or traffic to specific servers or applications, enabling informed capacity management.

<https://www.solarwinds.com/network-performance-monitor/use-cases/deep-packet-inspection>

The network packet analysis tools in NPM are designed to not only capture and analyze packet data, but they can also automatically classify network traffic. The platform is built to display network traffic information according to category and provide an estimate of the risk level associated with this traffic. The analyzer categorizes traffic according to elements like source or destination IP address, port usage, application type, and volume. Admins can also identify how traffic flows over a specific network link or to servers or applications. Armed with these insights, admins can make informed decisions about capacity planning. The network packet analysis tools in NPM can make it easier to filter out worrisome levels of non-business traffic.

<https://www.solarwinds.com/network-performance-monitor/use-cases/packet-analyzer>